

Egyéb

- Mit tehetek, ha elfogyott az adatforgalmi keretem?
- Mit tehetek ha a weboldalamat Bejelentett támadó webhelyként került megjelölésre?
- DotRoll tárhely biztonsági megoldások
- Időzített scriptek beállítása
- SSL
- Tárhely hosszabbítás megrendelése

Mit tehetek, ha elfogyott az adatforgalmi keretem?

Abban az esetben ha az adatforgalmi limit eléréséről értesítő emailt kapott akkor a <https://admin.dotroll.com> oldalon bejelentkezést követően lehetősége van kiegészítő adatforgalom vásárlására.

A megrendelés lépései:

1. Bejelentkezést követően kattintson a **Szolgáltatások / Szolgáltatásaim** menüpontra.
2. A baloldali oldalsávban található **További lehetőségek** dobozban kattintson a **Lehetséges kiegészítők** lehetőségre.
3. A megjelenő oldalon válassza ki a megvásárolni kívánt adatforgalmi csomagot, majd kattintson a **Megrendelés most** gombra.
4. Ezt követően kattintson az **Áttekintés** gombra, majd ellenőrizze le a számlázási adatokat.
5. Válassza ki a fizetési módot, valamint jelölje be az „Elovestam és elfogadom az Általános Szerződési Feltételeket” lehetőséget, és kattintson a **Megrendelés elküldése** gombra.

Mit tehetek ha a weboldalamat Bejelentett támadó webhelyként került megjelölésre?

Sajnos a bejelentett támadó webhellyel kapcsolatosan mi nem tudunk segíteni, mert ezt a típusú blokkolást nem mi helyeztük el, hanem a Google. Ez a típusú blokkolás hasznos hiszen így a látogató eszköze nem fertőződik meg, ugyanakkor elég kellemetlen.

A probléma megszüntetése érdekében végezze el az alábbi lépéseket:

1. Azon eszközök esetében ahonnan bejelentkezés történt a weboldalra, vagy a tárhelyre végezzen el víruskeresést.
2. Ezt követően jelentkezzen be a <https://admin.dotroll.com> oldalra és módosítsa a tárhely jelszavát, valamint az FTP felhasználók jelszavát.
3. Abban az esetben ha kapott CXS értesítést akkor az értesítő emailben szereplő fájlokat nézze át, ha nem a programkódhoz tartozó kódsorozatot talál a kódban akkor azokat távolítsa el. Ha valamilyen tartalom kezelő rendszert (CMS) használ akkor mindenképpen frissítse mind a tartalom kezelőt, mind a telepített kiegészítő modulokat, sablonokat. *Amennyiben nem Ön készítette a weboldalt akkor vegye fel a kapcsolatot a weboldal készítőjével, ugyanis programozással összefüggő kérdésekkel kapcsolatban nem fogunk tudni segítséget adni.*

A Google 90 naponként vizsgálja felül a honlapokat, amennyiben ezt nem kívánja kivárni akkor az alábbi lépések elvégzésével gyorsítható meg a blokkolás eltávolítása.

1. Ha a weboldal megtisztításra került a káros kódsorozatokról akkor, kérjük hogy olvassa el a [Google Search Console](#) súgóját.

Illetve a StopBadware oldalt amely angol nyelvű <http://www.stopbadware.org/>

2. Következő lépésként meg kell nézni a Google Diagnosztikai oldalát, amelyet így érhet el (végén a behelyettesítendő URL):

http://www.google.com/safebrowsing/diagnostic?site=http://az_on_domain_neve.tld

Figyelem: Az URL végén található az_on_domain_neve.tld részt cserélje ki arra a domain névre amelynél a probléma jelentkezik.

3. Ezután jelentkezzen be a [Google Webmaster Eszközökbe](#) ahol a felülvizsgálatot tudja kérvényezni.
4. Keressen rá oldalára a Badware Website Clearinghouse keresőjével (angol), majd a Report oszlopban szereplő linkekre kattintva kérje az oldalak felülvizsgálatát, bal oldalon felül a „Click to Request Review” linkekre kattintva.
<http://www.stopbadware.org/home/reportsearch>
5. Amennyiben phishing oldalként lett lejelentve, úgy kérjen az alábbi linken is felülvizsgálatot. http://sb.google.com/safebrowsing/report_error/

Várjon néhány napig, esetleg hétig, hogy a rendszereken átfusson a fertőzésmentesség híre, a sikerről a Webmaster Eszközökben is tájékoztatást küld majd.

Amennyiben bármilyen további kérdése van, forduljon Ügyfélszolgálatunkhoz bizalommal.

DotRoll tárhely biztonsági megoldások

A DotRoll fizetős tárhely építéskor nagy hangsúlyt fektettünk a szolgáltatás biztonságára, a felhasználók egymástól való védelmére. A teljesség igénye nélkül, ezek a következők:

RENDSZERFELHASZNÁLÓK

A szokványos tárhely-megoldásokkal ellentétben ügyfelenként külön rendszerfelhasználót hozunk létre, ezáltal a védelem már a rendszer magjában kezdődik. Ez lehetővé teszi számunkra, hogy a későbbiekben Önnek biztonságosan Perl és Python futtatási lehetőséget kínálhassunk.

PÁNCÉLOZOTT RENDSZERMAG

A rendszermagot különleges védelmmel láttuk el, ezért például a felhasználók nem láthatják egymás futó folyamatait és nem rabolhatnak a megengedettnél több erőforrást.

VIRTUÁLIS MINI KÖRNYEZET

Minden felhasználónak kialakításra kerül egy un. chroot környezet, amelyben egy teljesen működőképes Linux helyezkedik el. Minden felhasználó, akár FTP-n lép be, SSH-t használ vagy PHP alkalmazás fut, ebben a környezetben helyezkedik el és ebből kitörni nem tud. Ezáltal a felhasználók egymást semmilyen szinten nem láthatják.

KIMENŐ KAPCSOLATOK

Mivel egyre nagyobb szükség van különböző külső szolgáltatások (API-k) elérésére, a tárhelyet felszereltük az ezek eléréséhez szükséges eszközökkel (PHP SOAP, XML-RPC extension, stb). Az Ön védelme érdekében, esetleges betörések visszakövetését megkönnyítendő, a kimenő kapcsolatokat feljegyezzük.

E-MAIL KÜLDÉSI MEGOLDÁSOK

A lehető legnagyobb kompatibilitás elérésére a tárhelyről több módszerrel is lehet e-mail-t küldeni. A rendszer az Ön alkalmazásának teljesen transzparensen végzi a dolgát és szolgálja ki az e-mail-eket.

Mivel egyre nagyobb probléma olyan tárhelyet szerezni, amely kimenő levelező szervere nincs feketelistán, nagy hangsúlyt fektettünk arra, hogy egy-egy ügyfél csak a normális napi levelezési limitek keretében küldhessen e-mail-t kizárólag olyan domaint használva feladóként, amely tárhelye valóban a szolgáltatásunkat veszi igénybe. Ezen felül a kimenő leveleket digitális aláírással (DKIM) látjuk el, ami nagyon sok levelező szolgáltatás (pl Gmail) számára a megbízhatóság jele és a hagyományos e-mail küldéssel szemben vitathatatlaná teszi, hogy egy adott e-mail honnan származik.

Időzített scriptek beállítása

A beállításra két lehetőség is van.

1. Annál a fájlnál amelyet időzítetten szeretne futtatni a fájlra legalább a tulajdonosnak futtatási jogot kell beállítani (0700). Valamint a fájl elejére az (első sorban) kell megadni a fájl típusának megfelelő értelmezőt.**PHP fájl esetében:**

```
#!/usr/bin/php
```

Shell script esetében:

```
#!/bin/bash
```

Ebben az esetben a fájlt az időzített scriptek menüpontban elegendő megadni a következő formában: /home/username/public_html/cron.php

2. Az értelmezőt csak az Időzített scriptek menüpontban a futtatandó fájl előtt adja meg a következő formában:**PHP fájl esetében:**

```
php /home/username/public_html/cron.php
```

Shell script esetében:

```
/bin/sh /home/username/public_html/file.sh
```

Ez utóbbi esetben a fájlra nem kell beállítani futtatási jogot sem.

SSL

Az SSL/TLS egy olyan protokoll, amely biztonságos adatátvitelre szolgál. Amennyiben a kapcsolat két végpontja támogatja, szinte bármilyen más protokollt lehet SSL-en keresztül továbbítani.

Az SSL egy fontos tulajdonsága az aláírhatóság. A kulcsokat aláírhatjuk és így hitelesíthetjük. A szoftvergyártók (pl böngészők) a böngészőkbe ágyazva szállítanak egy listát az általuk elismert aláírókról, amely aláírását a szoftver automatikusan elfogadja. Egyéb esetekben a szoftver rákérdez a kulcs elfogadására.

Tárhely hosszabbítás megrendelése

A meghosszabbítás menete:

1. Jelentkezzen be a <https://admin.dotroll.com/> címen a számlafizetői fiók regisztrációjakor megadott email címmel.
2. Kattintson a felső menü sorban a **Szolgáltatások / Szolgáltatásaim** menü pontra.
3. A megjelenő oldalon kattintson a **További beállítások gombra** (*ne a lehulló listában található egyéb opciókra*)
4. Az oldal betöltését követően kattintson a *Automata hosszabbítás státusza: Igen* felirat alatt található **Szolgáltatás hosszabbítása azonnal 1 évvel** gombra.

A rendszerünk ezt követően elkészíti a díjbekérő számlát amely alapján az átutalást el tudja indítani.